Estruturando um CSIRT

A Experiência do NARIS

RICARDO KLÉBER

www.ricardokleber.com
ricardokleber@ricardokleber.com
@ricardokleber

Antes de mais nada..
É possível/viável montar um CSIRT?

- Motivando (ou desmotivando !!??)
  - Esse cenário é familiar para você?
    - Muito trabalho x pouca gente
    - Bolsistas x continuidade
    - Outras atividades da equipe (todo mundo faz tudo !!??)
    - Política de segurança mais abrangente x Instituição pública
    - Conscientização dos Usuários (Segurança x Usabilidade)



Antes de mais nada..

É possível/viável montar um CSIRT?

- Motivando (ou desmotivando !!??)

Você não está sozinho !!!

2º Fórum Brasileiro de CSIRTs

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Voltando um Pouquinho no Tempo...

1998

Check Point®
SOFTWARE TECHNOLOGIES LTD.

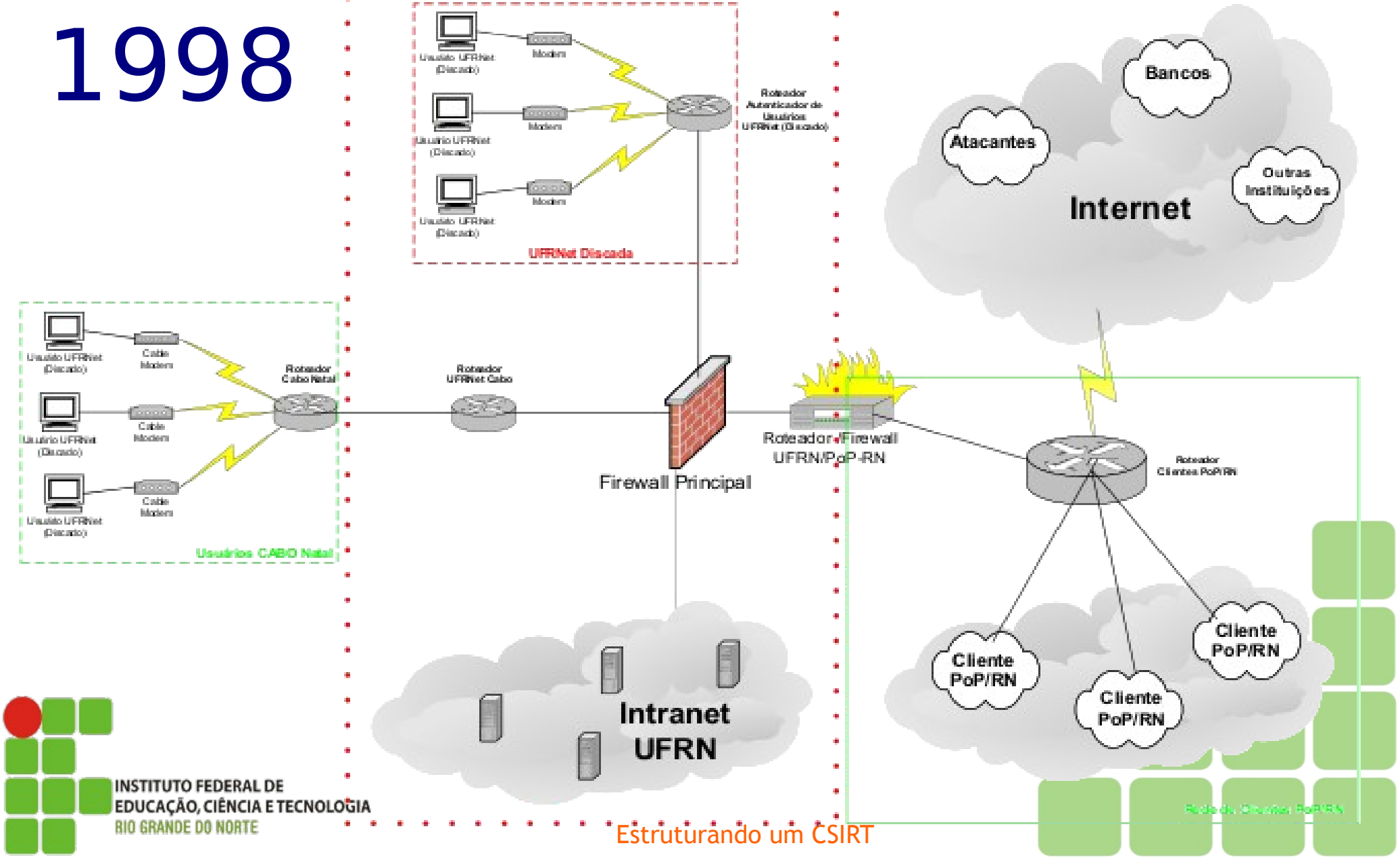
FireWall-1

- Ultra-1 (Sun Microsystems)
- Sistema Operacional Solaris
- Software Firewall-1

NARIS

Qual o Tamanho do “Problema” ?

1998



NARIS

Euquipe !!??

1998

Motivações para a Criação de uma Estrutura de Apoio

- Complexidade crescente dos sistemas (hardware e software)
- Grande número de vulnerabilidades
- Falso Positivos e Falso Negativos (variação de ataques)
- Facilidade em ocultar os passos de uma invasão
- Comunicação rápida e eficiente entre invasores

  (email, WEB, conferências, chats, etc)
- Legislação (ou falta de...)
- Mesmo problema resolvido de várias formas diferentes

Motivações para a Criação de uma Estrutura de Apoio

- Banalização do “Consultor de Segurança”
- “ex”-invasores vendendo “proteção”
- “saber” invadir = saber proteger?
- invasores com pouco nível de conhecimento
- ferramentas automáticas (e.g. rootkits)
- Falta de experiência/capacitação de equipes de TI
- Desatualização de sistemas operacionais e serviços
- Phishing... botnets... Crime Organizado na Internet...

Desafios Imediatos

- Manter o Ambiente e Gerenciar Incidentes de Segurança
  - Identificar, formalizar e gerenciar:
    - processos necessários para controlar/administrar as tarefas associadas com o tratamento de incidentes de segurança
    - serviços proativos e reativos, que auxiliam o processo de tratamento de incidentes de segurança

Preparação, Proteção, Detecção, Triagem e Resposta

Desafios Imediatos (por onde começar???)

- Na Prática...
  - Otimizar e “dominar” regras do Firewall
  - Instalar e manter um IDS de Rede (NIDS)
  - Manter atualizados os sistemas operacionais e serviços (servidores)
  - Monitorar logs e cruzar dados (Firewall / IDS / Servidores)
  - Responder a todos os incidentes reportados à instituição
  - Reportar incidentes a partir da análise (e triagem) de logs

Isso foi / é o básico !!!

Formalizando o CSIRT da UFRN

- Oficializado (fundação) em 01/11/2002
- Objetivo: Atuar na prevenção, investigação e resposta a incidentes de segurança no âmbito da rede UFRN

- Equipe Especializada:
  - Diminuição no tempo de detecção
  - Investigação criteriosa
  - Diminuição no tempo de resposta

NARIS

Prevenção contra Incidentes

- Acompanhamento de listas especializadas

  (novos tipos de ataque)

- Atualização de sistemas operacionais e serviços

  (sub-área específica)

- Cooperação com Administradores Locais

  (atingindo o usuário final)

- Testes de penetração

  (busca do “elo mais fraco”)

Investigação de Incidentes

- Padronização de procedimentos
  - Ataque interno? Ataque Externo? Spam? Worm? Virus?
  - Invasão? DoS/DDoS? Pixação? Fraude?
  - Preservação de “cena de crime”
  - Cópia fiel / Assinatura Hash
  - Necessidade de ajuda externa (PF / CAIS / CERT)?
  - Relatório
  - Sigilo !!!

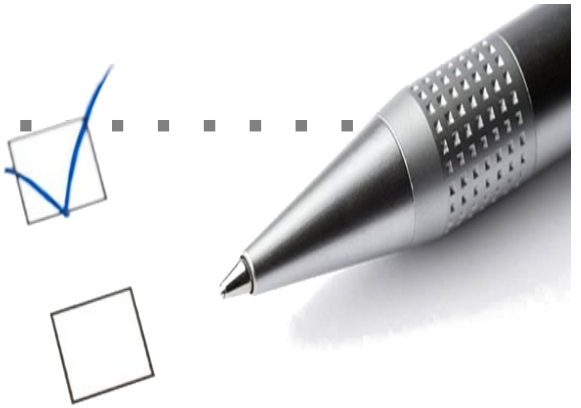
NARIS

Resposta a Incidentes

- Incidentes Internos → Identificação e processo administrativo
- Incidentes Externos
  - Identificação da rede remota (origem ou destino)
  - Notificação: Rede remota, CAIS, CERT, CSIRTS Específicos
  - Medidas restritivas de acesso
  - Cada caso analisado individualmente
  - Acionamento da polícia (quando for o caso)

NARIS

Áreas de Atuação



- Firewalls
- NIDS
- Atualização de Sistemas Operacionais e Serviços
- Servidor de Logs Centralizado (Loghost)
- Documentação das Atividades do Núcleo
- Serviços à Comunidade

NARIS

Áreas de Atuação

- Firewalls
  - Manutenção das regras de filtragens do FW Principal
  - Documentação de scripts e arquivos de configuração
  - Plano de contingência (eventual falha do Fw)
  - Análise de logs do firewall e respostas aos incidentes
- NIDS
  - Manutenção dos NIDS (DMZ e Intranet)
  - Análise de logs
  - Procedimentos reativos de notificação e regras no firewall
  - Implantação de outros IDS em segmentos críticos

NARIS

Áreas de Atuação

- Atualização de Sistemas Operacionais e Serviços
  - Acompanhamento contínuo de novas vulnerabilidades (listas de discussão, fóruns e “underground”)
  - Planejamento de atualizações de S.O. e serviços
  - Sondagens (testes de penetração) nos servidores internos
  - Identificação e desativação de serviços desnecessários
- Servidor de Logs Centralizado (Loghost)
  - Instalação, configuração e manutenção do Loghost
  - Redirecionamento dos logs de todos os servidores internos sob co-administração da equipe (+ shells modificadas).
  - Uso de ferramentas de análise de logs

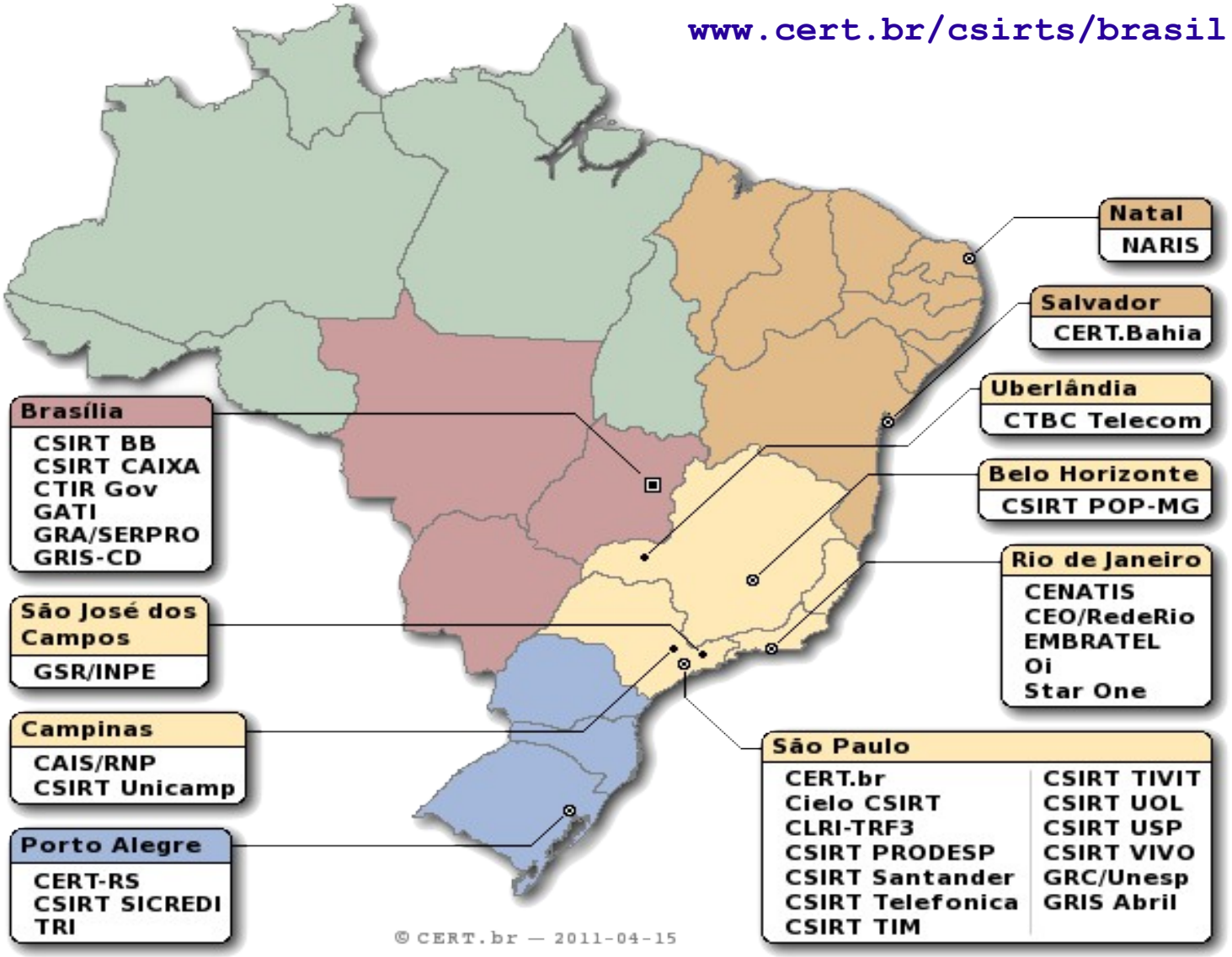
Áreas de Atuação

- Documentação das Atividades do Núcleo
  - Implementação de página web do NARIS
  - Atualização periódica dos dados:
    - Orientação aos usuários da rede
    - Resultados das atividades do núcleo
    - Gráficos estatísticos

- Serviços à Comunidade
  - Alertas de segurança nas listas internas da instituição
  - Cursos, palestras e disseminação da política de segurança
  - Apresentação dos resultados do núcleo à comunidade

Reconhecimento no Brasil

www.cert.br/csirts/brasil



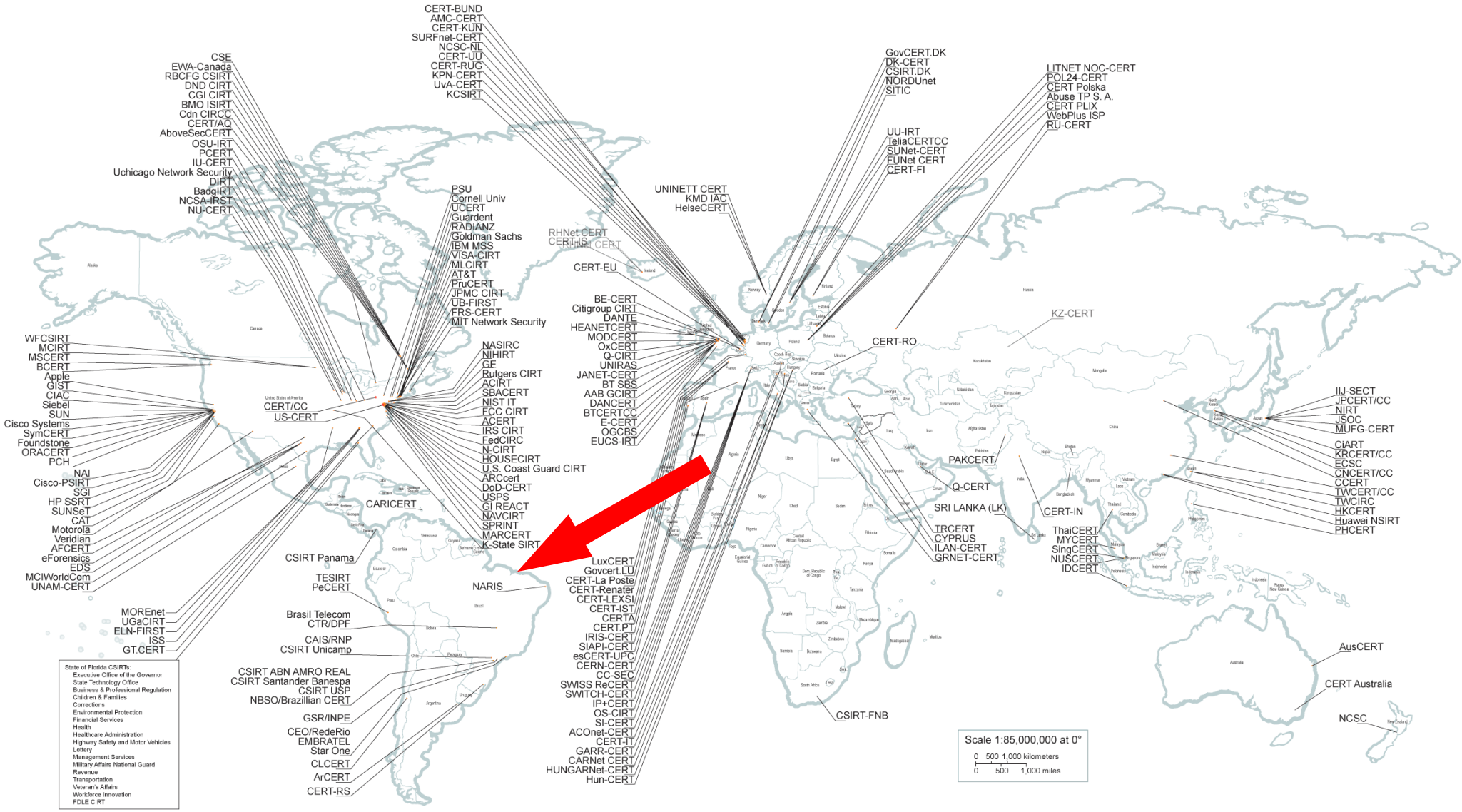
NARIS

www.cert.org/csirts

Reconhecimento no Mundo

Incident Response Teams Around the World

International cooperation speeds response to Internet security breaches.



NARIS

O Que Aprendemos (Recomendações Finais)

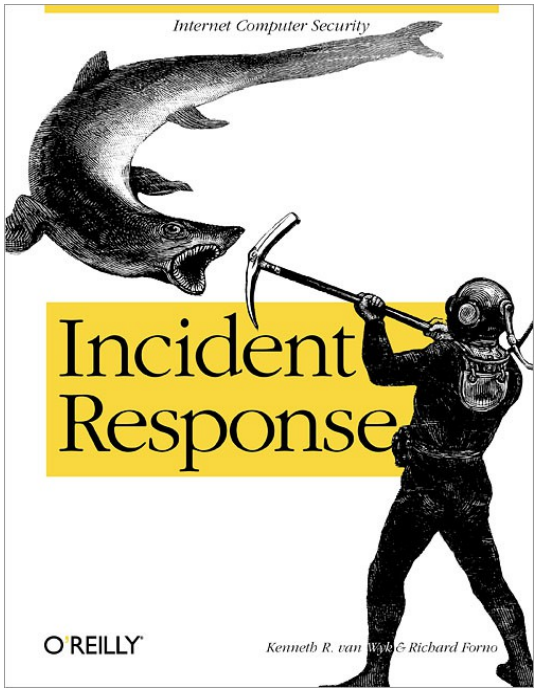
- Continuidade do Núcleo (CSIRT)
  - Buscar manter independência de pessoas
    - Tarefas sempre realizadas por (pelo menos) dois membros
  - Preparar substituição/sucessão de membros
  - Formalização do Núcleo e de sua Estrutura
  - Respaldo de Instância decisória (diretoria)
  - Programa de Estágio (preparação de novos analistas)
    - Cuidado com antecedentes (“ficha limpa”)

- Leitura Complementar
  - Incident Response

    Kenneth R. van Wyk,Richard Forno

    ISBN 0-596-00130-4

    http://oreilly.com/catalog/9780596001308/



Material de Apoio para CSI

www.cert.br/csirts/

Ir para o conteúdo

English

cert.br 15 ANOS

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

Núcleo de Informação e Coordenação do Ponto BR

CGI.br - NIC.br - Registro.br - CERT.br - CETIC.br - CEPTRO.br - W3C.br

Imprensa

Você está em: CERT.br > CSIRTs

- Sobre o CERT.br
- CSIRTs
- Estatísticas
- Cursos
- Projetos
- Publicações
- Palestras
- Links
- FAQ
- Mapa do site
- Contato
- Twitter
- RSS

Busca

Materiais de Apoio para Grupos de Resposta a Incidentes de Segurança em Computadores (CSIRTs)

CSIRTs no Brasil

- Lista de CSIRTs Brasileiros

CSIRTs no Mundo

- CSIRTs com Responsabilidade Nacional
- CSIRTs membros do FIRST
- Lista de CSIRTs Europeus
- CSIRTs da Ásia e Oceania membros do APCERT

Documentos em Português

- CERT/CC CSIRT FAQ (Tradução autorizada pelo SEI/CMU)
- Criando um Grupo de Respostas a Incidentes de Segurança em Computadores: Um Processo para Iniciar a Implantação (Tradução autorizada pelo SEI/CMU)
- Expectativas quanto a Grupos de Resposta a Incidentes de Segurança em Computadores

E hoje?

Novos Projetos...

www.eha.net.br

www.ricardokleber.com/videos

www.ricardokleber.com/palestras

ricardokleber@ricardokleber.com

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Estruturando um CSIRT

A Experiência do NARIS

RICARDO KLÉBER

www.ricardokleber.com
ricardokleber@ricardokleber.com
@ricardokleber